IN THE CLAIMS

Please replace any and all prior listings of the claims with the following replacement list.

Replacement List of Claims

1. (Currently amended) Apparatus for the secure installation and use of an information system comprising:

a plurality of nodes, where said plurality of nodes includes at least one information appliance and at least one security console,

at least one data-carrying object containing security-related data; and

a plurality of object receptacles that comprises a portion of one or more of said nodes, two or more of said object receptacles being connected to said security console, said data-carrying object being inserted into a selected one of said two or more object receptacles that reads out the security-related data, wherein said security console, based on said security-related data and said selected receptacle, establishes a network policy that determines a desired security configuration of said information system with respect to said information appliance and said security console ~~is based on said security-related data and said selected receptacle~~.

2. (Original) Apparatus as in claim 1, wherein said data-carrying object stores the security-related data in a form that can be read-out by one of an electrical sensor, an optical sensor, or a magnetic sensor.

3. (Previously presented) Apparatus as in claim 1, wherein said data-carrying object remains inserted in said selected receptacle for as long as the security configuration is desired to be in effect.

4. (Previously presented) Apparatus as in claim 1, wherein said data-carrying object is temporarily made readable by said selected receptacle in order to initiate said security configuration.

5. (Previously presented) Apparatus as in claim 1, wherein said information appliance has associated therewith the security-related data of said data-carrying object, and wherein the information appliance is intended to be used for indicating that the information appliance is one of a trusted information appliance or an untrusted information appliance.

6. (Previously presented) Apparatus as in claim 1, wherein said information appliance is given access to information system resources, including information, by inserting an additional data-carrying object associated with said security console into at least one receptacle that has an output that is coupled to said information appliance.

7. (Previously presented) Apparatus as in claim 1, wherein each of said information appliance and said security console have associated therewith first and second corresponding data-carrying objects, respectively, wherein said selected receptacle comprises a first receptacle, wherein the information appliance is intended to be used for indicating, from security-related data contained on said first data-carrying object associated with said information appliance, that the information appliance is one that is authorized to fulfil and originate requests for information system resources, and wherein a second one of said receptacles has an output coupled to said information appliance for indicating, from security-related data contained on said second data-carrying object associated with said security console, that said security console is authorized to fulfil and originate requests for information appliance resources, including information.

8. (Previously presented) Apparatus as in claim 1, wherein said data carrying object comprises a first one of first and second data-carrying objects that are obtained as a pair, wherein said selected receptacle comprises a first receptacle, wherein the information appliance is intended to be used for indicating, from security-related data contained on said first data-carrying object, that the information appliance is one that is authorized to fulfil and originate requests for information system resources, and wherein a second one of said receptacles has an output coupled to said information appliance for indicating, from security-related data contained on said second data-carrying object, that said security console is authorized to fulfil and originate requests for information appliance resources, including information.

9. (Previously presented) Apparatus as in claim 1, wherein said selected receptacle comprises a first receptacle, and wherein an insertion of the data-carrying object into said first receptacle indicates different security-related information than inserting the data-carrying object into a second one of said two or more receptacles.

10. (Previously presented) Apparatus as in claim 1, wherein said data-carrying object is one of a pair of data-carrying objects, and wherein the data-carrying objects in any given pair are the same shape, and no two data-carrying objects not in the same pair are the same shape.

11. (Previously presented) Apparatus as in claim 1, wherein said data-carrying object is one of a pair of data-carrying objects, and wherein the data-carrying objects in any given pair are imprinted with a same visible identification information, and no two data-carrying objects not in the same pair are imprinted with the same visible identification information.

12. (Previously presented) Apparatus as in claim 1, wherein said data-carrying object is one of a pair of data-carrying objects, and wherein the data-carrying objects in any given pair are fashioned so as to mechanically join together, and no two

data-carrying objects not in the same pair will not or are unlikely to mechanically join together.

13. (Previously presented) Apparatus as in claim 1, wherein said data-carrying object is one of a group of at least three data-carrying objects, and where access to a resource of said information appliance, including information, is obtained by providing one subset of data-carrying objects from said group to a receptacle associated with a requestor of the resource, and a disjoint set of data-carrying objects from said group is provided to the receptacles of the security console.

14. (Previously presented) Apparatus as in claim 13, wherein identifications of all individual data-carrying objects in the group can be ascertained by viewing the security console, even if some subset of the data-carrying objects are provided to said receptacle associated with a requestor of the resource.

15. (Previously presented) Apparatus as in claim 13, wherein a utilization of different disjoint subsets of the data-carrying objects in said group indicates different levels of trust to be granted to the requestor with respect to the resource.

16. (Previously presented) Apparatus as in claim 13, wherein a utilization of different disjoint subsets of the data-carrying objects in said group indicates different levels of authorization to be granted to the requestor with respect to the resource.

17. (Previously presented) Apparatus as in claim 13, wherein data-carrying objects in said group mechanically join together to form an assemblage, where the assemblage is adapted to be attached to a device through a single connection.

18. (Previously presented) Apparatus as in claim 1, wherein said information appliance is one of a group of information appliances, wherein a newly-obtained information appliance is added to said group on behalf of a principal, by providing an

additional data-carrying object representing the principal to a receptacle of the newly obtained information appliance.

19. (Previously presented) Apparatus as in claim 18, wherein said data-carrying object representing the principal contains data which includes at least one secret known only to the principal.

20. (Previously presented) Apparatus as in claim 19, wherein the secret known only to the principal comprises the private half of a public-private key pair associated with an asymmetric cryptosystem.

21. (Previously presented) Apparatus as in claim 1, wherein said information appliance is authorized on behalf of a certain principal, wherein said certain principal, and said information appliance is granted a certain level of access to a certain resource of said information appliance by providing, to one of said receptacles associated with said information appliance representing the resource, an additional data-carrying object representing the principal.

22. (Previously presented) Apparatus as in claim 21, wherein data contained in the additional data-carrying object representing the principal comprises the public half of a public-private key pair associated with an asymmetric cryptosystem.

23. (Previously presented) Apparatus as in claim 22, in which the additional data-carrying object representing the principal comprises an image of the principal.

24. (Previously presented) Apparatus as in claim 22, in which the additional data-carrying object representing the principal comprises a computer-readable data portion and an image of the principal.

25. (Original) Apparatus as in claim 24, further comprising a holder for holding the computer-readable data portion such that both the computer-readable data portion and the image are accessible.

26. (Currently amended) A method for the secure installation and use of an information system comprising a plurality of nodes, where said plurality of nodes include at least one information appliance and at least one security console, said method comprising steps of:

providing at least one data-carrying object containing security-related data; ~~and~~

inserting the data-carrying object into a selected one of a plurality of object receptacles that comprises a portion of at least one of the nodes, wherein the selected object receptacle is one of two or more of said receptacles that are connected to said security console, the data-carrying object being inserted into the selected receptacle that reads out the security-related data; and

based on the security-related data and the selected object receptacle, establishing a network security policy that determines ~~wherein~~ a desired security configuration of said information system with respect to said information appliance and said security console ~~is based on the security-related data and the selected object receptacle~~.

27. (Original) A method as in claim 26, wherein the data-carrying object stores the security-related data in a form that can be read-out by one of an electrical sensor, an optical sensor, or a magnetic sensor.

28. (Previously presented) A method as in claim 26, wherein the data-carrying object either remains inserted in the selected receptacle during the operation of the information system, or is temporarily inserted in or otherwise made readable by the selected receptacle either before or during the operation of the information system.

29. (Currently amended) A method as in claim 26, wherein said information appliance has associated therewith the security-related data of said data-carrying object, ~~whereinthe~~ wherein the information appliance is intended to be used for indicating that the information appliance is one of a trusted information appliance or an untrusted information appliance.

30. (Previously presented) A method as in claim 26, wherein said information appliance is given access to information system resources, including information, by inserting an additional data-carrying object associated with the security console into at least one of the receptacles that has an output that is coupled to the information appliance.

31. (Previously presented) A method as in claim 26, wherein each of the information appliance and the security console have associated therewith first and second corresponding data-carrying objects, respectively, wherein said selected receptacle comprises a first receptacle, wherein the information appliance is intended to be used for indicating, from security-related data contained on the first data-carrying object associated with the information appliance, that the information appliance is one that is authorized to fulfil and originate requests for information system resources, and wherein a second one of the receptacles has an output coupled to the information appliance for indicating, from security-related data contained on the second data-carrying object associated with the security console, that the security console is authorized to fulfil and originate requests for information appliance resources, including information.

32. (Previously presented) A method as in claim 26, wherein the data carrying object comprises a first one of first and second data-carrying objects that are provided as a pair, wherein the selected receptacle comprises a first receptacle, wherein the information appliance is intended to be used for indicating, from security-related data contained on said first data-carrying object, that the information appliance is one that is authorized to fulfil and originate requests for information system resources, and wherein a second one of the receptacles has an output coupled to the information appliance for

indicating, from security-related data contained on said second data-carrying object, that the security console is authorized to fulfil and originate requests for information appliance resources, including information.

33. (Previously presented) A method as in claim 26, wherein said selected receptacle comprises a first receptacle, and wherein an insertion of the data-carrying object into said first receptacle indicates different security-related information than inserting the data-carrying object into a second one of said two or more receptacles.

34. (Previously presented) A method as in claim 26, wherein the data-carrying object is one of a pair of data-carrying objects, and wherein the data-carrying objects in any given pair are the same shape, and no two data-carrying objects not in the same pair are the same shape.

35. (Previously presented) A method as in claim 26, wherein the data-carrying object is one of a pair of data-carrying objects, and wherein the data-carrying objects in any given pair are imprinted with a same visible identification information, and no two data-carrying objects not in the same pair are imprinted with the same visible identification information.

36. (Previously presented) A method as in claim 26, wherein the data-carrying object is one of a pair of data-carrying objects, and wherein the data-carrying objects in any given pair are fashioned so as to mechanically join together, and no two data-carrying objects not in the same pair will not or are unlikely to mechanically join together.

37. (Previously presented) A method as in claim 26, wherein said data-carrying object is one of a group of at least three data-carrying objects, and where access to a resource of the information appliance, including information, is obtained by providing one subset of data-carrying objects from said group to a receptacle associated with a

requestor of the resource, and a disjoint set of data-carrying objects from said group is provided to the receptacles connected to the security console.

38. (Previously presented) A method as in claim 37, wherein identifications of all individual data-carrying objects in the group can be ascertained by viewing the security console, even if some subset of the data-carrying objects are provided to the receptacle associated with a requestor of the resource.

39. (Previously presented) A method as in claim 37, wherein a utilization of different disjoint subsets of the data-carrying objects in said group indicates different levels of trust to be granted to the requestor with respect to the resource.

40. (Previously presented) A method as in claim 37, wherein a utilization of different disjoint subsets of the data-carrying objects in said group indicates different levels of authorization to be granted to the requestor with respect to the resource.

41. (Previously presented) A method as in claim 37, wherein data-carrying objects in said group mechanically join together to form an assemblage, where the assemblage is adapted to be attached to a device through a single connection.

42. (Previously presented) A method as in claim 37, in which access to the resource is denied unless every data-carrying object of the group is inserted into a receptacle.

43. (Previously presented) A method as in claim 26, wherein said information appliance is one of a group of information appliances, and further comprising a step of adding a newly-obtained information appliance to said group on behalf of a principal, by inserting an additional data-carrying object representing the principal to a receptacle of the newly obtained information appliance.

44. (Original) A method as in claim 43, wherein the data-carrying object representing the principal contains data which includes at least one secret known only to the principal.

45. (Original) A method as in claim 44, wherein the secret known only to the principal comprises the private half of a public-private key pair associated with an asymmetric cryptosystem.

46. (Currently amended) A method as in claim 26, wherein said information ~~applicance~~ appliance is authorized on behalf of a certain principal, wherein said certain principal, and said information appliance is granted a certain level of access to a certain resource of said information appliance by inserting, to one of said receptacles associated with the information appliance representing the resource, an additional data-carrying object representing the principal.

47. (Previously presented) A method as in claim 46, wherein data contained in the additional data-carrying object representing the principal comprises the public half of a public-private key pair associated with an asymmetric cryptosystem.

48. (Previously presented) A method as in claim 47, in which the additional data-carrying object representing the principal comprises an image of the principal.

49. (Previously presented) A method as in claim 47, in which the additional data-carrying object representing the principal comprises a computer-readable data portion and an image of the principal.

50. (Original) A method as in claim 49, further comprising a step of providing a holder for holding the computer-readable data portion such that both the computer-readable data portion and the image are accessible.

51. (Currently amended) A computer program embodied on a computer-readable medium for providing for the secure installation and use of an information system comprising a plurality of nodes, where said plurality of nodes include at least one information appliance and at least one security console, said computer program comprising code segments responsive to at least one data-carrying object containing security-related data that is inserted into a selected one of a plurality of object receptacles that comprises a portion of at least one of the nodes, wherein the selected object receptacle reads out the security related data and is one of two or more of said object receptacles that are connected to said security console, and wherein, based on said security-related data and said selected receptacle, one or more of said code segments cause said security console to establish a network policy that determines a desired security configuration of said information system with respect to said information appliance and said security console ~~is based on said security-related data and said selected receptacle~~.

52. (Currently amended) Apparatus for the secure installation and use of an information system comprising:

a plurality of nodes, where said plurality of nodes includes at least one information appliance and at least one security console,

at least first and second physical data-carrying objects each containing security-related data; and

a first object receptacle and a second object receptacle that are connected to said security console, a third object receptacle connected to said information appliance, said first physical data-carrying object being inserted into a selected one of said first and second object receptacles that reads out the associated security-related data, said second physical data-carrying object being inserted into said third object receptacle that reads out associated security-related data, wherein, based on said security-related data and said selected one of said first and

second object receptacles, said security console establishes a network policy that determines a desired security configuration of said information system ~~is based on said security-related data and said selected one of said first and second object receptacles~~, and wherein said security configuration gives access to a resource of one of said information system by said information appliance and said information appliance by said security console.